FAA National Software Conference, May 2002
The IISAP/IISEE Process

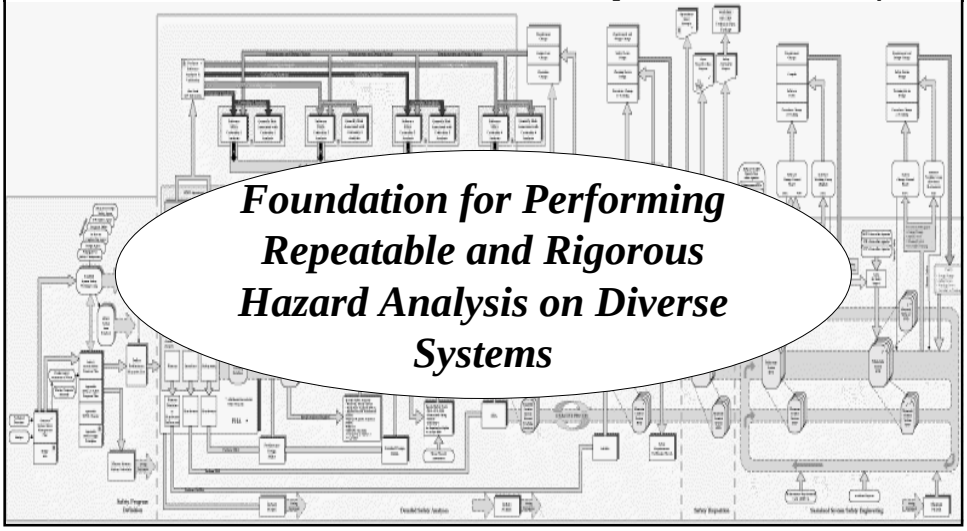
Integrated Safety Engineering Environment (ISEE)

Presented by:

Ron Stroup AIO 200
Warren Naylor BAE Systems

The IISAP/ISEE Process

Four Phase Process Which When Documented and Implemented Will Provide for a …



FAA National Software Conference, May 2002
The IISAP/IISEE Process

Why IISAP?

- To Improve Quality of Safety Programs
  - Cost & Schedule
  - Quality Control of Safety Products
  - Clear Guidelines
  - Common Terminology
  - Common Methodology
  - Incompatibilities Between Interfacing Safety Programs (End-To-End System Safety)
  - Hazard Identification
  - Residual Risk Definition, Communication and Acceptance
  - Training to Produce Qualified System Safety Engineers

How Does IISAP Improve System Safety Engineering?

- Provides Consistent and Well Defined System Safety Methodology and Terminology For Application Across Programs
- Improves Overall Quality & Technical Accuracy of Safety Analyses and Review Board Presentations
- Provides Guidance and Training for New Safety Engineers
- Provides Framework for Definition and Communication of Residual Risk to Decision Makers
- Approaches Safety as a Systems Engineering Discipline
- CMM/iCMM Compatible

IISAP Milestones

Where We've Been

- IISAP Integration Team Initiated August 2000
- Process Briefed Up through NAVSEA Dahlgren Technical Director
- Requirements Have Been Derived and Formally Approved
- Endorsed by Weapon System Explosives Safety Review Board as "Best Practice" for Navy System Safety Programs
- Briefed the FAA's System Safety Working Group
- The FAA agreed to become an active partner in the tools development

Where We Are

- Adopted IPT Structure
- Developing IISAP Data Elements
- Initiated Development of IISAP Database and Training Tools

IISAP Milestones

Where We're Going

- Fully Develop IISAP/ISEE and Train System Safety Engineers
- Pursue Government Patents of IISAP Tools
- Present IISAP at International System Safety Conference and Other Services
- Fully Implement within the FAA, NAVSEA and DoD

IISAP Development Background

- ***IISAP Development is Based Upon:***
  - The FAA's System Safety Management Plan (SSMP)
  - Mil-STD-882C/D *(Standard Practice for System Safety)*
  - DoD 5000.2-R *(Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information System Acquisition Programs)*
  - OD 44942 *(Weapons System Safety Guidelines Handbook)*
  - Joint Software System Safety Handbook
  - Combat System Safety Engineering Branch, Industry and Academic Technical Expertise

Common Problem, Common Solution

DoD Implementation

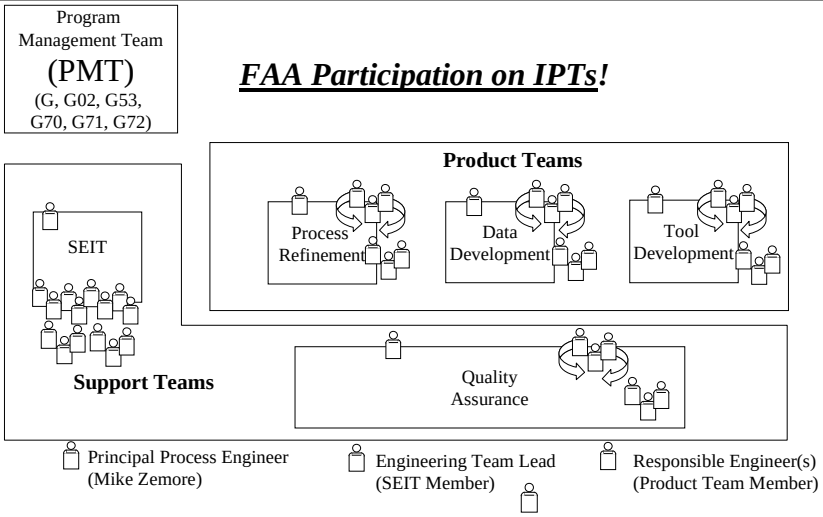
- ©Integrated Interoperable Safety Analysis Process (IISAP)
  - IISAP is the foundation for performing repeatable and rigorous hazard analysis on diverse systems by providing system safety analysts, tools and guidance on analysis techniques, quality control and defensible residual risk assessments.

FAA Implementation

- **Integrated Safety Engineering Environment (ISEE)**
  - Mission Need Statement: Develop a tool that will facilitate the management of system safety activities, training of safety professionals, and execution of the Safety Risk Management (SRM) process of the FAA National Airspace System (NAS)

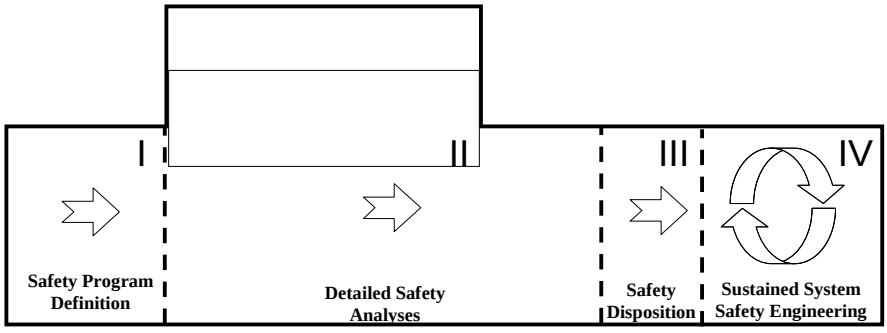
© NSWCDD has applied for a patent to be owned by the Government.

IISAP Development IPT Structure

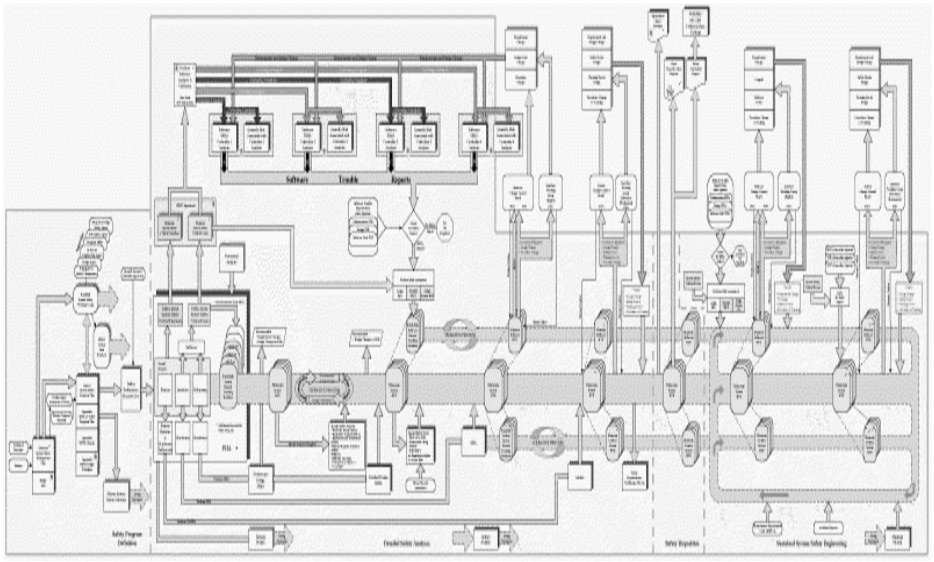


IISAP - Process Overview

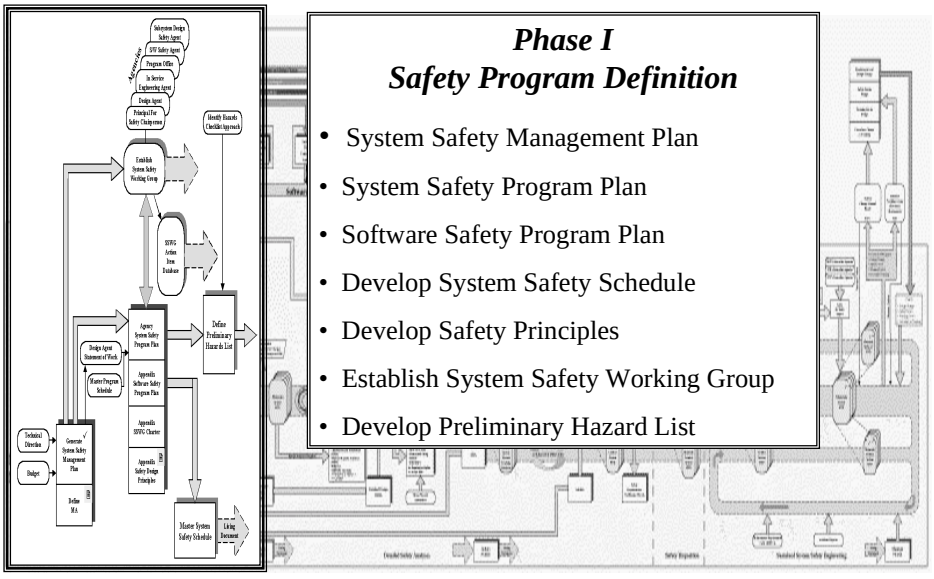
Four Basic Phases...



IISAP - Process Overview



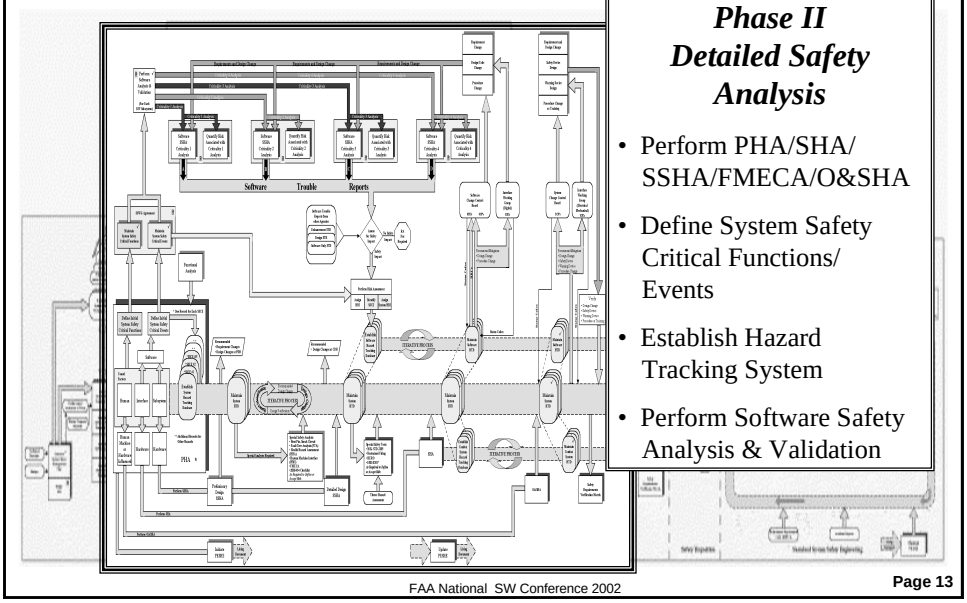
IISAP - Process Overview



Phase I
Safety Program Definition

- System Safety Management Plan
- System Safety Program Plan
- Software Safety Program Plan
- Develop System Safety Schedule
- Develop Safety Principles
- Establish System Safety Working Group
- Develop Preliminary Hazard List

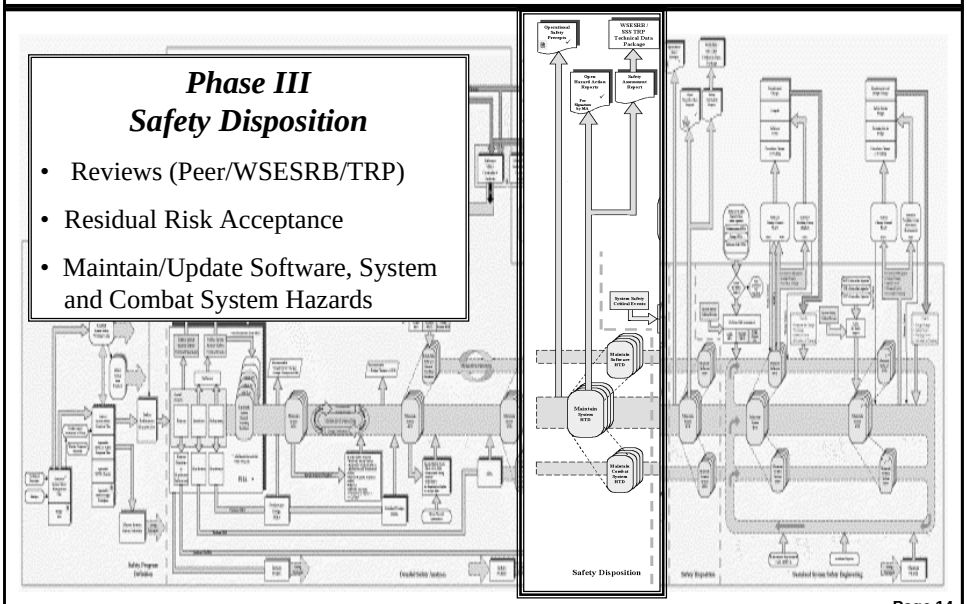
IISAP - Process Overview



Phase II
Detailed Safety Analysis

- Perform PHA/SHA/ SSHA/FMECA/O&SHA
- Define System Safety Critical Functions/ Events
- Establish Hazard Tracking System
- Perform Software Safety Analysis & Validation

IISAP - Process Overview

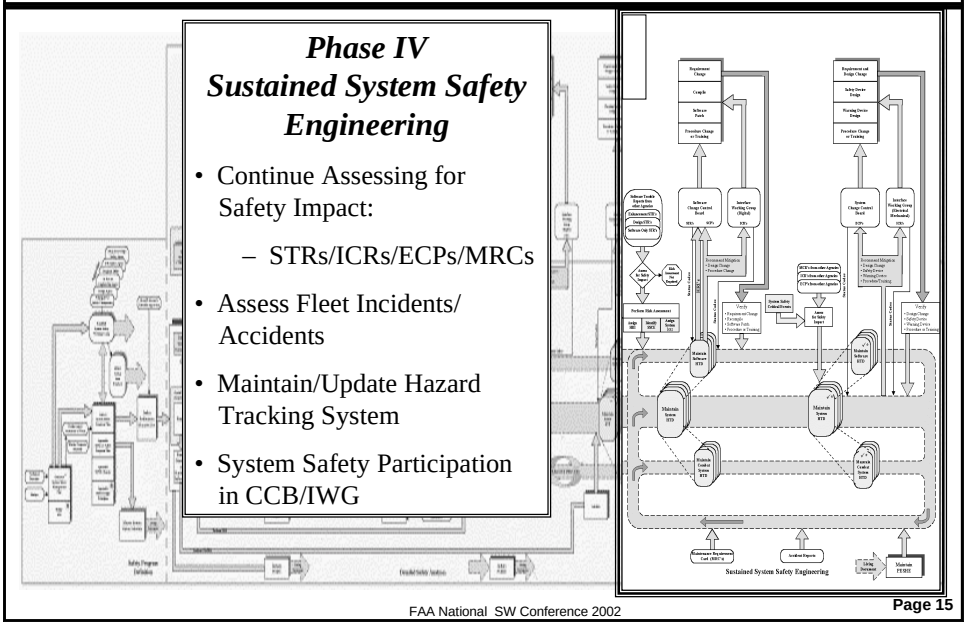


Phase III
Safety Disposition

- Reviews (Peer/WSESRB/TRP)
- Residual Risk Acceptance
- Maintain/Update Software, System and Combat System Hazards

FAA National Software Conference, May 2002
The IISAP/IISEE Process

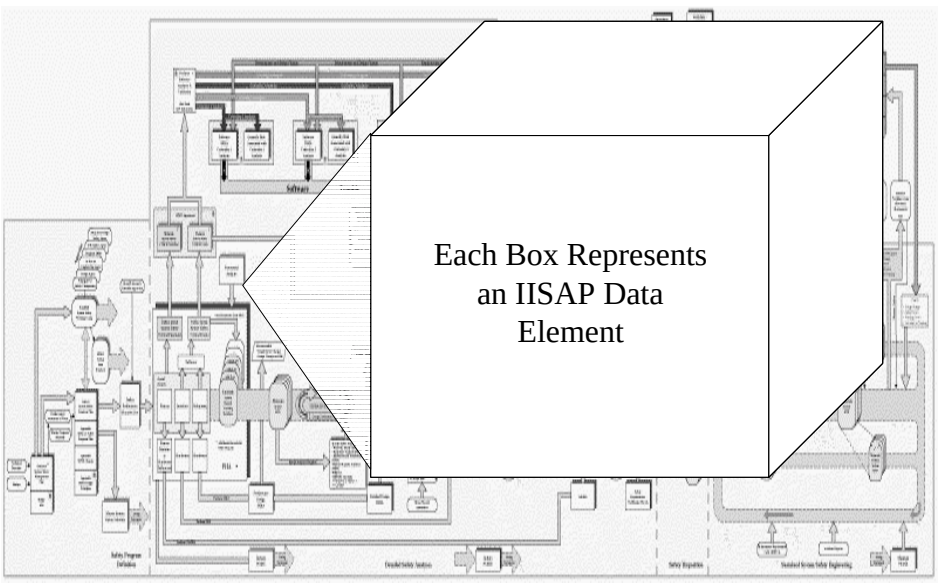
IISAP - Process Overview



Phase IV
Sustained System Safety Engineering

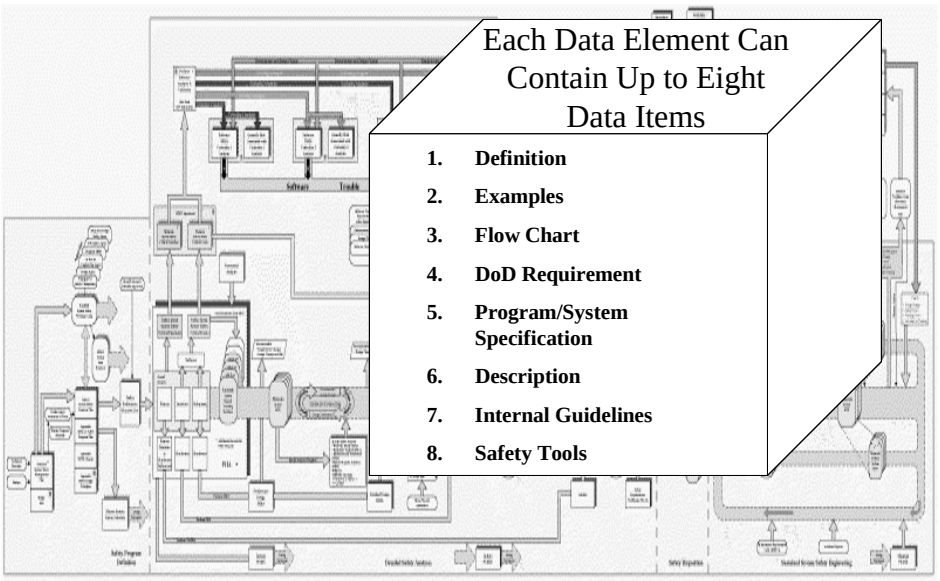
- Continue Assessing for Safety Impact:
  - STRs/ICRs/ECPs/MRCs
- Assess Fleet Incidents/ Accidents
- Maintain/Update Hazard Tracking System
- System Safety Participation in CCB/IWG

IISAP Tool



FAA National Software Conference, May 2002
The IISAP/IISEE Process

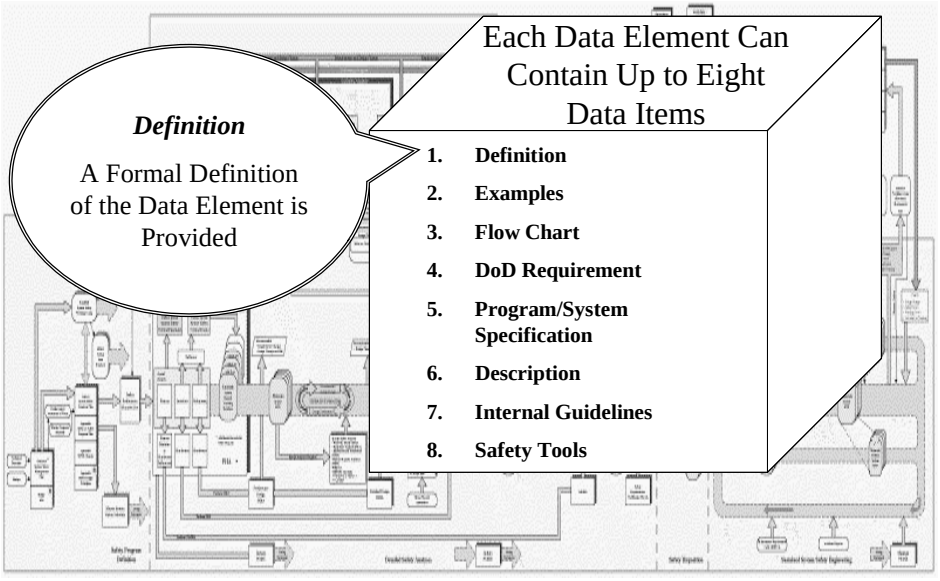
IISAP Tool



FAA National SW Conference 2002

Page 17

IISAP Tool

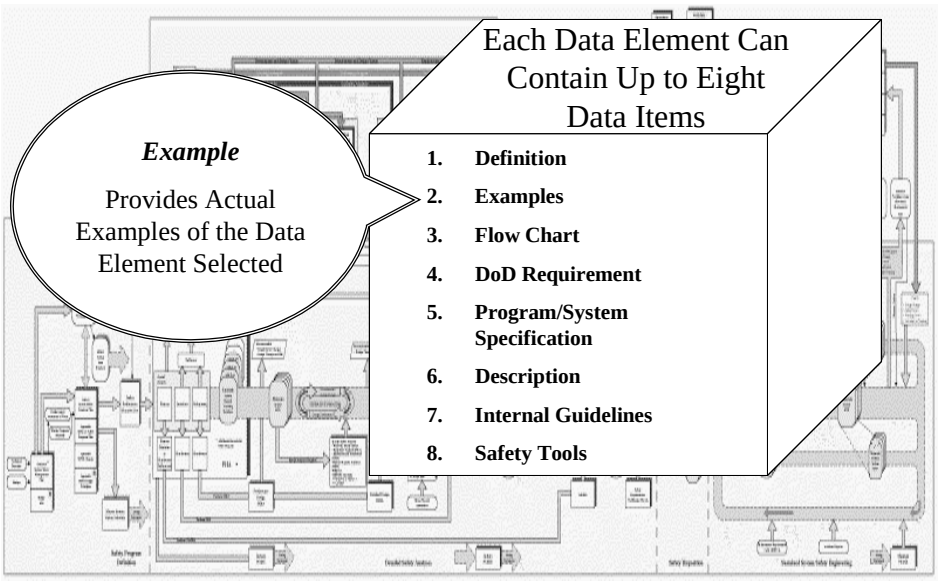


FAA National SW Conference 2002

Page 18

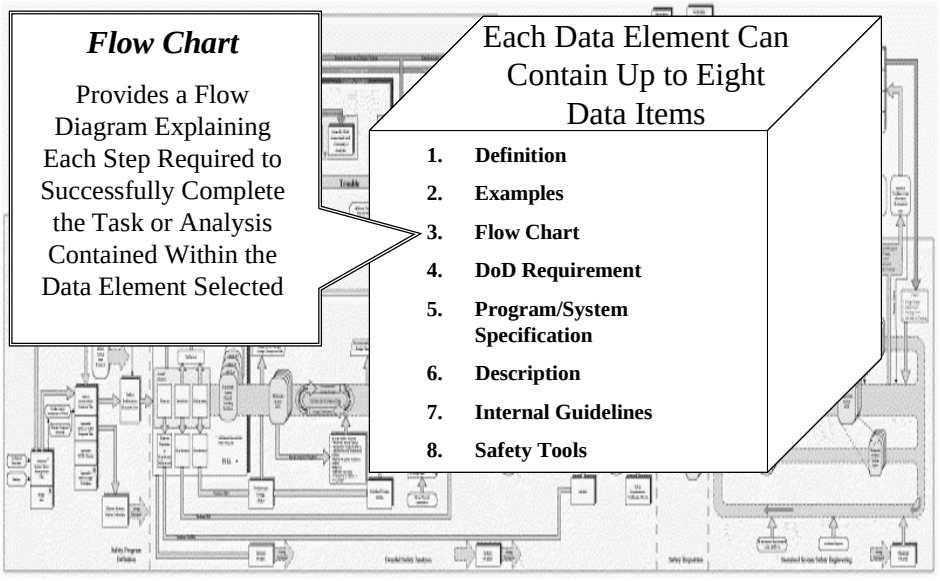
FAA National Software Conference, May 2002
The IISAP/IISEE Process

IISAP Tool



FAA National SW Conference 2002 Page 19

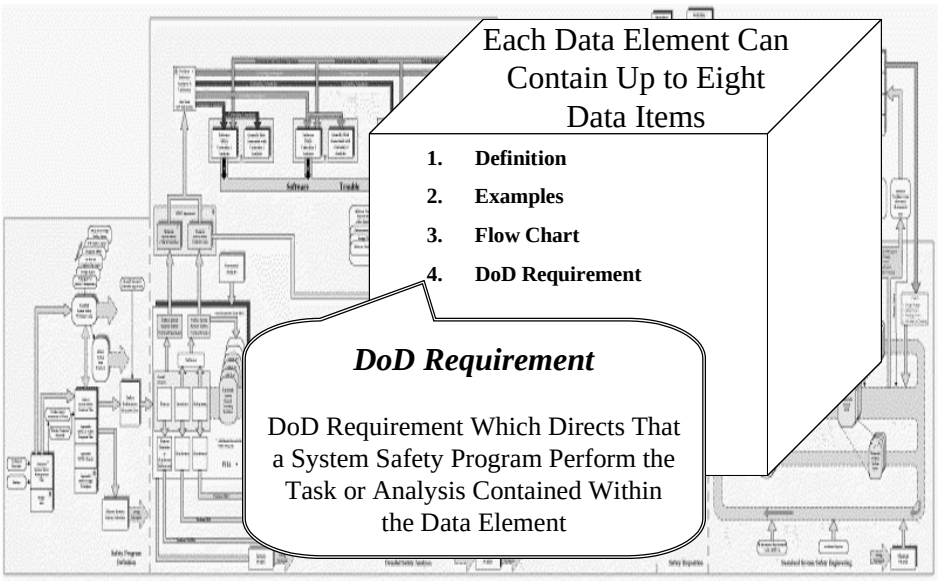
IISAP Tool



FAA National SW Conference 2002 Page 20

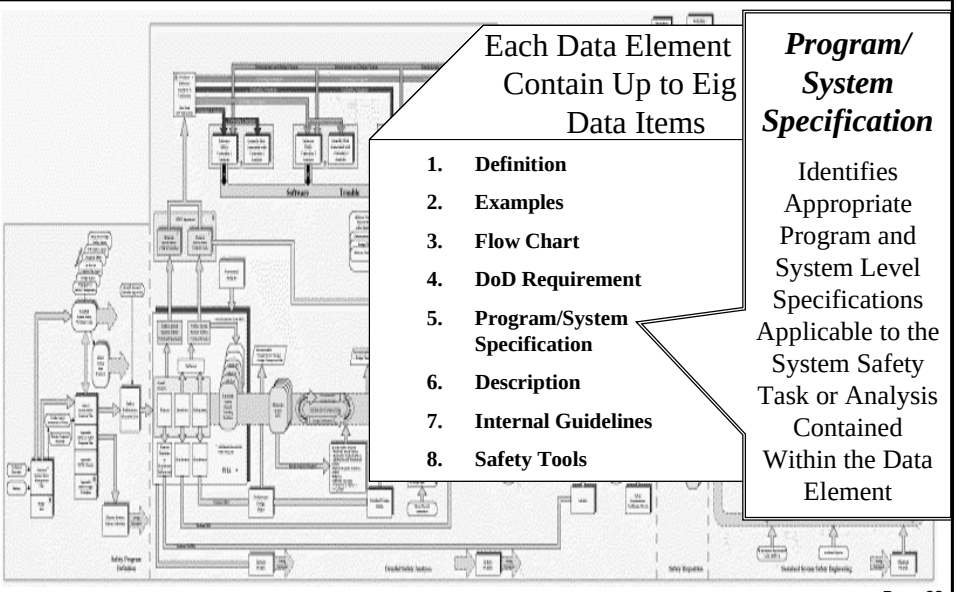
FAA National Software Conference, May 2002
The IISAP/IISEE Process

IISAP Tool



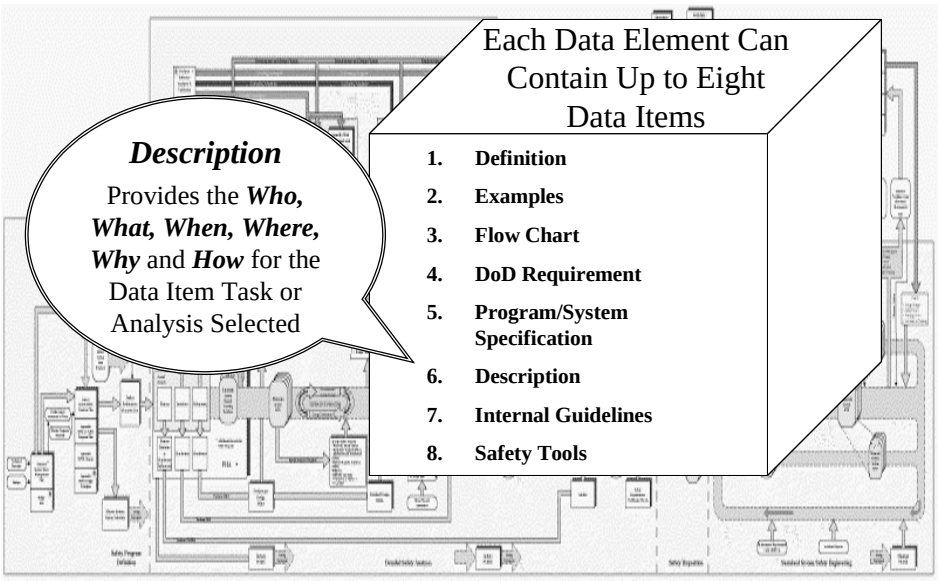
FAA National SW Conference 2002 Page 21

IISAP Tool



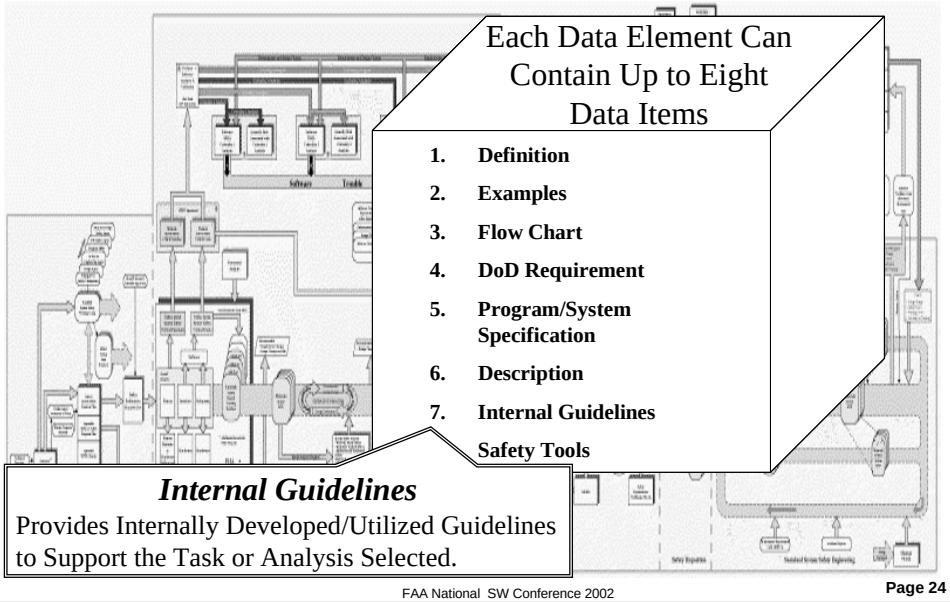
FAA National SW Conference 2002 Page 22

IISAP Tool



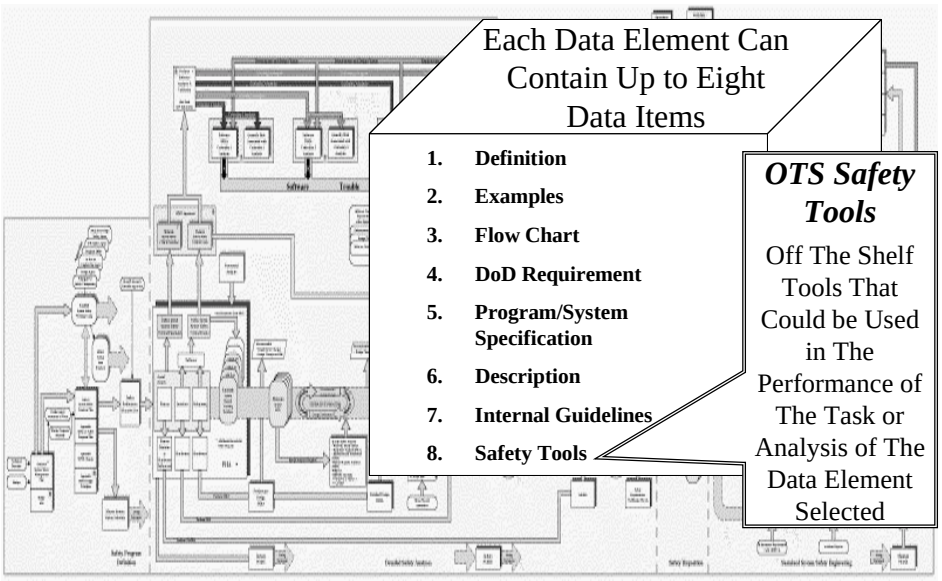
FAA National SW Conference 2002 Page 23

IISAP Tool



FAA National SW Conference 2002 Page 24

IISAP Tool



Each Data Element Can Contain Up to Eight Data Items

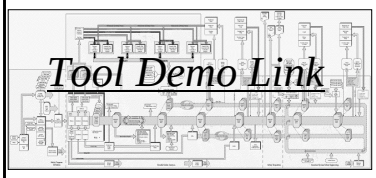
1. **Definition**
2. **Examples**
3. **Flow Chart**
4. **DoD Requirement**
5. **Program/System Specification**
6. **Description**
7. **Internal Guidelines**
8. **Safety Tools**

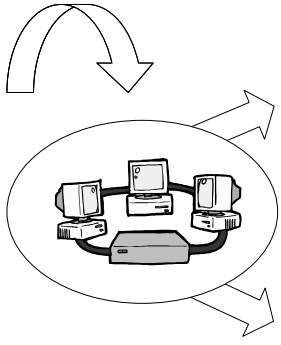
OTS Safety Tools

Off The Shelf Tools That Could be Used in The Performance of The Task or Analysis of The Data Element Selected

IISAP Tool Deployment

IISAP Process





Server/Web Based Training of System Safety Engineers

Provides for Mobility and Training of SE Without Server Access

Summary

- IISAP Will Provide for a Comprehensive, Technical Accurate, Repeatable and Supportable System Safety Process
- IISAP Allows for Continuous Process Improvement
- IISAP Will be a Significant Tool For the Training and Development of System Safety Engineers

IISAP Will Result in the Deployment of Safer Systems

Points of Contact (FAA)

- Scott Van Buren,
- Ron Stroup, AIO 200
- Gene Rice, ADSTSTECH

Points of Contact (DoD)

- Mike Zemore, Code G71
  - ZemoreMG@nswc.navy.mil Phone 540.653.8878
- Brad Cobb, Code G71
  - CobbBR@nswc.navy.mil Phone 540.653.8171
- Robert Stiegler, Code G70
  - StieglerRL@nswc.navy.mil Phone 540.653.7802
- Joe Janney, Code G71
  - JanneyJT@nswc.navy.mil Phone 540.653.3408